PATENT ABSTRACTS OF JAPAN

(11)Publication number : **09-160832**

(43)Date of publication of application : **20.06.1997**

(51)Int.Cl. **G06F 12/14**

G06F 3/06

G06F 12/16

(21)Application number : **07-317894** (71)Applicant : **HITACHI LTD**

(22)Date of filing : **06.12.1995** (72)Inventor : **DOMYO SEIICHI**

KURODA SAWAKI

KAMIYAMA ZENSHI

(54) **METHOD AND SYSTEM FOR BACKING UP AND RESTORING DATA**

(57)Abstract:

PROBLEM TO BE SOLVED: To keep backup data secret by receiving a deciphering key for restoring data on a portable medium (tape) from a 2nd computer and deciphering the data on the portable medium with the received deciphering key.

SOLUTION: This system is equipped with a 1st computer 101 on which the tape 100 where the backup data are stored can be loaded, a restorer terminal 102 connected to the 1st computer 101, a 2nd computer 104 connected to the 1st computer 101 through a network 103, and an administrator terminal 105

connected to the 2nd computer 104. When the backup data stored on the tape 10 are restored, a user DB 106 and a restorer DB 107 arranged on the side of the 2nd computer 104 are used to authorize the user and restorer on-line and only the user who is registered as a regular user or restorer is allowed to decipher the data on the tape 100.

LEGAL STATUS

[Date of request for examination]	06.09.1999
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3481755
[Date of registration]	10.10.2003
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	10.10.2006

CLAIMS

[Claim(s)]

[Claim 1] The 1st computer which restores the backed up data while backing up

data to a portable medium, They are the data backup / the restoration approach in the distributed system equipped with the 2nd calculating machine connected to this 1st calculating machine via the network. The step which inputs at least one person's restoration person identification information which allows the reconstitution of data which backs up in case data are backed up to a portable medium by said 1st calculating machine, The step which inputs the cryptographic key of the data which back up, and the step which detects the identifier of a portable medium, The step made to register into the database which sends 1 set of information which consists of the identifier, the restoration person identification information, and the cryptographic key of said portable medium to the 2nd calculating machine, and the 2nd calculating machine manages, The step which enciphers the data for backup by said cryptographic key, and is stored in said portable medium, The step which inputs a restoration person's identification information in case the 1st computer restores the backup data enciphered from said portable medium, By transmitting the step which detects the identifier of the portable medium for restoration, and the identifier of a portable medium and a restoration person's identification information to the 2nd calculating machine, and collating with the information in said database The step from which a restoration person receives authentication of whether to be the restoration person of the normal beforehand registered into the database, The data backup / the restoration approach characterized by having the step which inputs the decode key for receiving the authentication result of the purport which is the restoration person of normal, and restoring the data of a portable medium, and the step which decodes the data of a portable medium with the inputted decode key.
[Claim 2] The 1st computer which restores the backed up data while backing up data to a portable medium, They are the data backup / the restoration approach in the distributed system equipped with the 2nd calculating machine connected to this 1st calculating machine via the network. The step which inputs at least one person's restoration person identification information which allows the reconstitution of data which backs up in case data are backed up to a portable

medium by said 1st calculating machine, The step which inputs the cryptographic key of the data which back up, and the step which detects the identifier of a portable medium, The step made to register into the database which sends 1 set of information which consists of the identifier, the restoration person identification information, and the cryptographic key of said portable medium to the 2nd calculating machine, and the 2nd calculating machine manages, The step which enciphers the data for backup by said cryptographic key, and is stored in said portable medium, The step which inputs a restoration person's identification information in case the 1st computer restores the backup data enciphered from said portable medium, By transmitting the step which detects the identifier of the portable medium for restoration, and the identifier of a portable medium and a restoration person's identification information to the 2nd calculating machine, and collating with the information in said database By the authentication result of the step from which a restoration person receives authentication of whether to be the restoration person of the normal beforehand registered into the database, and the purport which is the restoration person of normal The data backup / the restoration approach characterized by having the step which receives the decode key for restoring the data of a portable medium from the 2nd calculating machine, and the step which decodes the data of a portable medium with the received decode key.

[Claim 3] For the portable medium which backs up data, 1 set of information which consists of the identifier, the restoration person identification information, and the cryptographic key of said portable medium is the data backup / the restoration approach according to claim 1 or 2 characterized by recording on a different portable medium and sending to the manager of the 2nd calculating machine.

[Claim 4] 1 set of information which consists of the identifier, the restoration person identification information, and the cryptographic key of said portable medium is the data backup / the restoration approach according to claim 1 or 2 characterized by said thing [transmitting to the 2nd calculating machine via a

network, and registering with said database by processing of the 2nd calculating machine].

[Claim 5] In the distributed system equipped with the 1st computer which restores that backed up data, and the 2nd computer connected to this 1st computer via the network while backing up data to the portable medium A means by which said 1st calculating machine inputs at least one person's restoration person identification information which allows the reconstitution of data which backs up, A means to input the cryptographic key of the data which back up, and a means to detect the identifier of a portable medium, The means made to register into the database which sends 1 set of information which consists of the identifier, the restoration person identification information, and the cryptographic key of said portable medium to the 2nd calculating machine, and the 2nd calculating machine manages, A means to encipher the data for backup by said cryptographic key, and to store in said portable medium, By transmitting an input means to input the identification information of the restoration person who restores the backup data enciphered from said portable medium, and the identifier of a portable medium and a restoration person's identification information to the 2nd calculating machine, and collating with the information in said database A means by which a restoration person receives authentication of whether to be the restoration person of the normal beforehand registered into the database, A means to input the decode key for receiving the authentication result of the purport which is the restoration person of normal, and restoring the data of a portable medium, It has a means to decode the data of a portable medium with the inputted decode key. Said 2nd computer A means to register into a database 1 set of information which consists of the identifier, the restoration person identification information, and the cryptographic key of the portable medium sent from said 1st computer, By collating with the identifier of a portable medium and a restoration person's identification information which received from the 1st calculating machine, and the information in said database The distributed system characterized by having a means by which a restoration person attests whether

you are the restoration person of the normal beforehand registered into the database, and answers the 1st computer via a network in the authentication result.

[Claim 6] In the distributed system equipped with the 1st computer which restores that backed up data, and the 2nd computer connected to this 1st computer via the network while backing up data to the portable medium A means by which said 1st calculating machine inputs at least one person's restoration person identification information which allows the reconstitution of data which backs up to a portable medium, A means to input the cryptographic key of the data which back up, and a means to detect the identifier of a portable medium, The means made to register into the database which sends 1 set of information which consists of the identifier, the restoration person identification information, and the cryptographic key of said portable medium to the 2nd calculating machine, and the 2nd calculating machine manages, A means to encipher the data for backup by said cryptographic key, and to store in said portable medium, By transmitting a means to input the identification information of the restoration person who restores the backup data enciphered from said portable medium, and the identifier of a portable medium and a restoration person's identification information to the 2nd calculating machine, and collating with the information in said database By the authentication result of a means by which a restoration person receives authentication of whether to be the restoration person of the normal beforehand registered into the database, and the purport which is the restoration person of normal It has a means to receive the decode key for restoring the data of a portable medium from the 2nd calculating machine, and a means to decode the data of a portable medium with the received decode key. Said 2nd calculating machine A means to register into a database 1 set of information which consists of the identifier, the restoration person identification information, and the cryptographic key of the portable medium sent from said 1st computer, By collating with the identifier of a portable medium and a restoration person's identification information which received from the 1st calculating

machine, and the information in said database The distributed system which attests whether a restoration person is a restoration person of the normal beforehand registered into the database, and is characterized by having a means to answer the 1st computer via a network in the decode key for restoration only when it is the restoration person of normal.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to data backup / the restoration approach, and a system, and relates to the data backup / the restoration approach, and system for the ability not to restore the backup data especially stored in the portable medium to an inaccurate user.

[0002]

[Description of the Prior Art] The data backup approach in a calculating-machine technique is business which restores data based on the contents of the tape, when the data of a calculating machine are periodically stored in portable media (it is hereafter described as a tape), such as a magnetic tape and a magnetic disk, and use of the data on a calculating machine becomes improper by factors, such as failure generating.

[0003] However, compared with the calculating-machine top by which OS (operating system) attests a user, it is mentioned as a trouble of this backup activity that possibility that an inaccurate user will access the data of a tape is high.

[0004] Then, in the case of backup, a user is made to input a cryptographic key, and after enciphering the data stored in a tape by the cryptographic key, there is a method of storing the enciphered data in a tape.

[0005] If the key for decode corresponding to a cryptographic key is not inputted, since the data of a tape cannot be decoded according to this approach, the secret nature or the safety of data stored in the tape can be raised.
[0006] In addition, the key for decode has a private key method using the same thing as a cryptographic key, and a open code **** method using another thing.
[0007] Thus, there are Simson Garfinkel, Gene Spafford work, the Yamaguchi English translation, "UNIX security", and (ASCII:1993) as reference of the well-known technique which enciphers to the data for backup.
[0008] The distributed system using the computer of a large number arranged in a network is increasing so that it may be represented with vocabulary called the Internet and WWW with change of the use gestalt of a computer in recent years. Also in such a distributed system, the data backup using a data encryption means is required as mentioned above.
[0009] When carrying out data backup in a distributed system, the following poses a problem.
[0010] (1) In a distributed system, a computer may become thousands of sets of scales, and, in such a case, an operator and a restoration person become a multiple name. Therefore, since the user (it is hereafter described as an operator) who backs up data, and the user (it is hereafter described as a restoration person) who restores data may not be the same person, storage of the key for decode in such a case and delivery become troublesome. Moreover, with the employment gestalt which manages a cryptographic key and a decode key off-line on an operator's responsibility, management of a decode key becomes complicated. When a cryptographic key and a decode key are stolen, it becomes impossible furthermore, to hold the secret nature of data.
[0011] (2) Since a calculating machine other than the backed up calculating machine may restore the data on a tape, it is necessary to define the authentication approach of the user in that case.
[0012] (3) Transmitting backup data including the secrecy of a cryptographic key, user information, and business on a network, even if it has enciphered avoids as

much as possible.

[0013] It is introducing OS which attests the user of an alien machine, and middleware about the matter of the above (2) with reference to the user DB on the computer which a system administrator's manages severely, and can solve. For example, it is the technique called OSF/DCE and they are Ward Rosenberry and David Kenney & Gerry Fisher. It is indicated by work, Understanding DCE, O'Reilly &Associates, and Inc (1992).

[0014] Moreover, in order to avoid tapping and the alteration on a network about the matter of the above (3), it is solvable by the employment approaches, such as sending of the tape by the vendor.

[0015]

[Problem(s) to be Solved by the Invention] However, about the matter of (1) mentioned above, the effective well-known technique which solves this is not found.

[0016] Without doing the troublesome delivery activity and the storage activity of the key for decode, the purpose of this invention allows only the decode person of normal whom the operator accepted decode of backup data, and is to offer the data backup / the restoration approach, and system which can hold the secret nature of backup data.

[0017]

[Means for Solving the Problem] For the above-mentioned purpose achievement, the data backup approach of this invention The step which inputs at least one person's restoration person identification information which allows the reconstitution of data which backs up in case data are backed up to a portable medium by said 1st calculating machine, The step which inputs the cryptographic key of the data which back up, and the step which detects the identifier of a portable medium, The step made to register into the database which sends 1 set of information which consists of the identifier, the restoration person identification information, and the cryptographic key of said portable medium to the 2nd calculating machine, and the 2nd calculating machine manages, The step which

enciphers the data for backup by said cryptographic key, and is stored in said portable medium, The step which inputs a restoration person's identification information in case the 1st computer restores the backup data enciphered from said portable medium, By transmitting the step which detects the identifier of the portable medium for restoration, and the identifier of a portable medium and a restoration person's identification information to the 2nd calculating machine, and collating with the information in said database The step from which a restoration person receives authentication of whether to be the restoration person of the normal beforehand registered into the database, It is characterized by having the step which inputs the decode key for restoring the data of a portable medium, and the step which decodes the data of a portable medium with the inputted decode key in response to the authentication result of the purport which is the restoration person of normal.

[0018] In this case, the authentication result of the purport which is the restoration person of normal can receive the decode key for restoring the data of a portable medium from the 2nd calculating machine, and it can constitute so that the data of a portable medium may be decoded with that received decode key.

[0019] Moreover, it can transmit to the 2nd computer via the approach of recording on a different portable medium from the portable medium which backs up data, and sending to the manager of the 2nd computer, or a network, and the approach of registering into said database by processing of the 2nd computer can be used for 1 set of information which consists of the identifier, the restoration person identification information, and the cryptographic key of a portable medium.

[0020] Moreover, when not attested as a restoration person of normal, while stopping restoration of a portable medium, it can constitute so that the manager of a system may be notified of the unauthorized use of a portable medium.

[0021] Moreover, before backing up data to a portable medium, the identifier of a portable medium is detected and the identifier and a backup operator's identifier are sent to the 2nd calculating machine, and after checking that it is not the

portable medium which the others enciphered, it can constitute so that backup may be started.

[0022] The system which realizes the data backup / the restoration approach of above-mentioned this invention It has the 1st computer which restores data, and the 2nd computer connected to this 1st computer via the network. Said 1st computer A means to input at least one person's restoration person identification information which allows the reconstitution of data which backs up, A means to input the cryptographic key of the data which back up, and a means to detect the identifier of a portable medium, The means made to register into the database which sends 1 set of information which consists of the identifier, the restoration person identification information, and the cryptographic key of said portable medium to the 2nd calculating machine, and the 2nd calculating machine manages, A means to encipher the data for backup by said cryptographic key, and to store in said portable medium, By transmitting an input means to input the identification information of the restoration person who restores the backup data enciphered from said portable medium, and the identifier of a portable medium and a restoration person's identification information to the 2nd calculating machine, and collating with the information in said database A means by which a restoration person receives authentication of whether to be the restoration person of the normal beforehand registered into the database, A means to input the decode key for receiving the authentication result of the purport which is the restoration person of normal, and restoring the data of a portable medium, It has a means to decode the data of a portable medium with the inputted decode key. Said 2nd computer A means to register into a database 1 set of information which consists of the identifier, the restoration person identification information, and the cryptographic key of the portable medium sent from said 1st computer, By collating with the identifier of a portable medium and a restoration person's identification information which received from the 1st calculating machine, and the information in said database It is characterized by having a means by which a restoration person attests whether you are the restoration person of the normal

beforehand registered into the database, and answers the 1st computer via a network in the authentication result.

[0023]

[Embodiment of the Invention] Hereafter, the gestalt of implementation of operation of this invention is explained to a detail with reference to a drawing.

[0024] Drawing 1 is the system configuration Fig. showing the operation gestalt of the distributed system which enforces the data backup approach of this invention.

[0025] The 1st computer 101 by which the distributed system of this operation gestalt can equip with the tape 100 which stores backup data, or the already stored tape, The restoration person terminal 102 connected to this 1st computer 101, and the 1st computer 101 and the 2nd computer 104 connected by the network 103 course, In case the backup data which were equipped with the manager terminal 105 connected to this 2nd calculating machine 104, and were stored in the tape 100 are restored The user DB106 and those [restoration / DB107] who have been stationed at the 2nd computer 104 side are used, user authentication and restoration person authentication are performed on-line, and decode of the data of a tape 100 is permitted only to those who are registered as the user or restoration person of normal.

[0026] Here, the tape 202 which stored backup data has the volume ID 1001 and the data area 1002 which identify the tape concerned uniquely to the interior.

[0027] Moreover, the 1st calculating machine 101 has a backup program 1011 and OS1012 with communication facility, and has the data encryption program 1013 further.

[0028] The user check program 1014, the restoration person check program 1015, the cryptographic key manager 1015, the medium controlling mechanism 1016, and the restoration program 1017 are included in OS1012.

[0029] By inputting an invocation command at the restoration person terminal 102, a user or a restoration person starts the restoration program 1017 or the data encryption program 1013, and performs the backup process or the backup

reconstitution of data of data to a tape 100.

[0030] On the other hand, the 2nd computer 104 is equipped with OS1041 connected through a network 103 between OS's1012 of the 1st computer 101, and the user authentication server program 1042 which performs user authentication and the restoration person authentication server program 1043 which performs restoration person authentication.

[0031] The user ID 108 for a user to identify whether you are the person of the normal registered beforehand is stored in a user DB106.

[0032] 1 set of information which consists of the cryptographic key 1083 for restoring the restoration person ID 1082 who, on the other hand, shows the restoration person DB270 the restoration person of normal to whom the volume ID 1081 for identifying a tape 100 and restoration of the tape concerned were permitted, and the backup data of the tape concerned is beforehand stored according to the volume ID of a tape 100.

[0033] Here, the restoration person ID 1082 in the restoration person DB270 can register two or more persons per tape 100.

[0034] The backup process and data restoration processing in the system constituted as mentioned above are explained using the flow chart of drawing 2 .

[0035] backup **** -- a user starts a backup program 1011 through the restoration person terminal 102 first. A backup program 1011 calls the user check program 220, in order to check whether a user is a person of normal before starting a backup process.

[0036] The user check program 1014 calls the user authentication server 1042 of the 2nd calculating machine 104 through the communication facility and the network 103 of OS1012. And a restoration person transmits the user ID who inputted from the restoration person terminal 102.

[0037] The user authentication server 1042 acquires these two or more users ID 108 beforehand registered into DB106 from a user DB106. And if it investigates whether there is any match with the user ID whom the user inputted from the restoration terminal 102 this time and a match is in the user ID 108, the user

concerned will attest with his being the user of normal (step 200).

[0038] While notifying that to a backup program 1001 since it is an unauthorized use person if the user ID in agreement is not registered, it displays that he is an unauthorized use person on the screen of the restoration person terminal 102, and processing is stopped [subsequent] to a backup program 1001.

[0039] When it is checked that he is the user of normal, a user is notified of a backup program 1001 through the restoration person terminal 102 so that predetermined wearing opening may be equipped with a tape 100.

[0040] Then, if the attested user equips predetermined wearing opening with a tape 100 according to the operator guidance of a backup program 1001, backup book processing will be started.

[0041] In this backup book processing, the volume ID 1001 of a tape 100 is first read through the medium controlling mechanism 1016 (step 211).

[0042] Next, it is directed on the screen of the restoration person terminal 102 that a backup program 1011 inputs a user's cryptographic key (step 212).

[0043] If a cryptographic key is inputted, a backup program 1011 will transmit the inputted cryptographic key to the data encryption program 1013, will make the data which should back up to this encryption program 1013 encipher (step 212), and will be made to store in a tape 100 (step 214). In this case, the backup data which should be enciphered are stored in the memory which is not illustrated.

[0044] In the data encryption program 1013, registration of a restoration person is performed after termination of backup book processing. In this case, a user is asked for the reply of whether a restoration person exists in addition to the user who carried out the backup process. When for example, a backup operator also permits restoration to the subordinate's section chief and the chief by the manager, other restoration persons ID (or restoration person name) whom the user itself accepts from the restoration person terminal 102 are inputted from the restoration person terminal 102 there (step 220,221).

[0045] A backup program 1011 performs processing for registering into the restoration person DB107 the information on the volume ID of the tape 1100

obtained at the above step, the restoration person ID, and a cryptographic key.

[0046] As the registration approach to the restoration person DB107, information is stored in the approach of performing by the manual entry from the manager terminal 105, and the card (for example, a floppy disk = FD) which conveys information simply, the card is sent to the manager of the 2nd computer, and there are two methods of registering the information in a card to the restoration person DB107 by actuation of a manager.

[0047] When the approach of storing the information on Volume ID, the restoration person ID, and a cryptographic key in a card (for example, a floppy disk = FD), and storing in the restoration person DB107 there is chosen by the user, a backup program 1011 detects that predetermined wearing opening of the restoration person terminal 102 was equipped with the card, and stores the information on Volume ID, the restoration person ID, and a cryptographic key in the card (step 231,232).

[0048] A user sends the card to a manager (step 233).

[0049] the manager who received the card equips predetermined wearing opening of a manager terminal with the card (or -- inserting), makes the information in a card read, and makes it register to the restoration person DB107 through the restoration person authentication server 1043 of the 2nd calculating machine 104 (step 234,235)

[0050] When the method of registering the information on Volume ID, the restoration person ID, and a cryptographic key by the manual entry is chosen by the user, a user is notified of the information on Volume ID, the restoration person ID, and a cryptographic key by the approach of displaying or printing. A user goes to the installation of the manager terminal 105, and does the manual entry of the information on this notified volume ID, the restoration person ID, and a cryptographic key from the manager terminal 105. Or I contact a manager and have a manager do a manual entry (step 236).

[0051] 1 set of information which changes from the volume ID 1081 and those [restoration / ID] 1082 who backed up on the tape 100 this time, and a

cryptographic key 1083 to the restoration person DB107 by this is stored according to Volume ID.

[0052] Backup reconstitution-of-data processing, next the backup reconstitution-of-data processing stored in the tape 100 are explained.

[0053] First, a restoration person starts the restoration program 1017 through the restoration person terminal 102. The restoration program 1017 calls the user check program 1014, in order to check whether a restoration person is a user of normal before starting restoration processing.

[0054] The user check program 1014 calls the user authentication server 1042 of the 2nd calculating machine 104 through the communication facility and the network 103 of OS1012. And a restoration person transmits the restoration person ID who inputted from the restoration person terminal 102.

[0055] The user authentication server 1042 which received the restoration person ID acquires these two or more users ID 108 beforehand registered into DB106 from a user DB106. And if it investigates whether there is any match with the restoration person ID who received from the 1st computer 101 and a match is in the user ID 108, the restoration person concerned will attest with his being the user of normal (step 250).

[0056] If the user ID in agreement is not registered, since it is an unauthorized use person, that is notified to the user check program 1014 of the 1st computer 101, and the restoration program 1017 through the communication facility and the network 103 of OS10412, it displays that he is an unauthorized use person on the screen of the restoration person terminal 102, and restoration processing is stopped [subsequent] to the restoration program 1017 (step 271). Furthermore, to the manager terminal 105, the mail 1044 of a purport is transmitted by the unauthorized use person, the message of a purport is displayed on the screen of the manager terminal 105 by the unauthorized use person, and a manager is notified (step 272).

[0057] When it is checked that he is the user of normal (step 260), a restoration person is notified of the restoration program 1017 through the restoration person

terminal 102 so that predetermined wearing opening may be equipped with a tape 100.

[0058] Then, if the attested restoration person equips predetermined wearing opening with a tape 100 according to the operator guidance of the restoration program 1017, restoration book processing (step 280) will be started.

[0059] In this restoration book processing, the volume ID 1001 of a tape 100 is first read through the medium controlling mechanism 1016 (step 281).

[0060] Next, the restoration program 1017 calls the restoration person check program 1015.

[0061] In order to acquire the restoration person ID corresponding to the volume ID 1001 of a tape 100, the restoration person check program 1017 calls the restoration person authentication server 1043 of the 2nd calculating machine 104 through the communication facility and the network 103 of OS1012, attests it at the volume ID 1001 and step 250 of a tape 100 which were acquired at step 281, and transmits a restoration person's user ID.

[0062] The restoration person authentication server 1043 acquires two or more restoration persons ID 1082 corresponding to volume ID 1001 from the restoration person DB107 through this restoration person authentication server 1043. That is, two or more restoration persons ID 1082 whom the backup operator accepts beforehand are acquired.

[0063] And if it investigates whether there is any match with the user ID who attested at step 250 and a match is in the restoration person ID 1082, the restoration person concerned will attest with his being the restoration person of normal whom the backup operator accepts beforehand (step 282,283). In this case, the user ID who attested at step 250 may be made to acquire from the user authentication server 1042.

[0064] If the restoration person ID 1082 in agreement is not registered, since it is an unjust restoration person, that is notified to the data encryption program 1013 and the restoration program 1017, it displays that he is an unauthorized use person on the screen of the restoration person terminal 102 by the restoration

program 1017, and restoration processing is further stopped [subsequent] to the data encryption program 1013 (step 291). Moreover, transmit the mail 1044 of a purport by the unauthorized use person also to the manager terminal 105, a purport makes the screen of the manager terminal 105 carry out a message indicator by the unauthorized use person, and a manager is notified (step 292).

[0065] When it is checked that he is the restoration person of normal (step 283), it is directed on the screen of the restoration person terminal 102 that the decode program 1017 inputs a decode key (the same key as a cryptographic key) (step 284).

[0066] If a decode key is inputted, the decode key will be transmitted to the data encryption program 1013. The data encryption program 1013 decodes the data stored in the tape 100 through the medium controlling mechanism 1016 by read-out, decodes the read-out data with a decode key (step 285), and passes it to the restoration program 1017.

[0067] Thereby, the data which were enciphered by the data area 1002 of a tape 100 and were stored in it are restored (step 286).

[0068] Drawing 3 shows the relation of the program in the case of steps 250 and 260 in drawing 2 , and processing of 270. Especially, inside the halt processing of step 270, it is shown that the user authentication server 1042 transmits the stop order of restoration processing to the restoration program 1017, and is transmitting mail of a purport to the manager terminal 105 by the unauthorized use person with mail 1044 further.

[0069] Drawing 4 shows the relation of the program in the case of steps 282 and 283 in drawing 2 , and processing of 290. Especially, inside the halt processing of step 290 shows that the restoration person authentication server 1043 transmits the stop order of restoration processing to the data encryption program 1013, and is transmitting mail of a purport to the manager terminal 105 by the unauthorized use person with mail 1044 further.

[0070] As mentioned above, in case data are backed up on a tape 100, while enciphering by the cryptographic key as which the backup operator specified the

data for backup and storing in a tape 100 in this operation gestalt ID of two or more restoration persons whom the backup operator permitted "activation of restoration processing", In case Volume ID and the cryptographic key of the tape 100 which stored backup data are registered into the restoration person DB whom the system administrator has managed and the data of a tape 100 are restored ID of two or more restoration persons who are 1 set in the volume ID of a tape 100 Read-out, When it investigates whether the restoration person ID who is in agreement with ID which those who are going to restore inputted exists and the restoration person ID in agreement exists Those who are going to restore attest with his being the restoration person of normal who had "activation of restoration processing" accepted by the backup operator, and are made to allow decode for the encryption data of a tape 100 with the decode key which the restoration person inputted.

[0071] Therefore, after teaching a cryptographic key (decode key) beforehand to those who accept "activation of restoration processing", a backup operator If ID of those who accept the "activation of restoration processing" is registered into the restoration person DB107 Only the decode person of normal whom the backup operator itself accepted can be made to restore the backup data of a tape 100, without performing troublesome delivery of a cryptographic key (decode key). It prevents that backup data leak to the outsider whom the backup operator does not accept, and it becomes possible to hold the secret nature of backup data.

[0072] In addition, in case restoration processing is performed, those who are going to restore are made to input a decode key, but since the cryptographic key 1083 is registered into the restoration person DB107 with the restoration person ID, it may be made to carry out the code of the encryption data by this cryptographic key 1083. It becomes unnecessary in this case, for a backup operator to teach a cryptographic key (decode key) beforehand to those who accept "activation of restoration processing."

[0073] Although it registers with the restoration person DB (database) whom the

backup operator inputted the cryptographic key, stored in the card (for example, floppy disk), and the manager of a distributed system has managed with the 2nd operation gestalt above-mentioned operation gestalt of this invention, a cryptographic key and the restoration person ID can also be registered through a network 103 by using the e-mail and RPC (remote pro SEJA call) of transmit data which are enciphered and sent.

[0074] Drawing 5 is a flow chart which shows the procedure of registering a cryptographic key and the restoration person ID into the restoration person DB107 of the 2nd calculating machine 104 by network 103 course.

[0075] First, a user (backup operator) starts a backup program 1011 through the restoration person terminal 102. A backup program 1011 calls the user check program 1014, in order to check whether a user is a user of normal before starting a backup process.

[0076] The user check program 1014 calls the user authentication server 1042 of the 2nd calculating machine 104 through the communication facility and the network 103 of OS1012. And a user transmits the user ID who inputted from the restoration person terminal 102.

[0077] The user authentication server 1042 which received User ID acquires these two or more users ID 108 beforehand registered into DB106 from a user DB106. And if it investigates whether there is any match with the user ID who received from the 1st computer 101 and a match is in the user ID 108, the user concerned will attest with his being the user of normal (step 501).

[0078] If the user ID in agreement is not registered, since it is an unauthorized use person, that is notified to the user check program 1014 of the 1st calculating machine 101, and a backup program 1011 through the communication facility and the network 103 of OS1042, it displays that he is an unauthorized use person on the screen of the restoration person terminal 102, and a backup process is stopped [subsequent] to a backup program 1011. Furthermore, to the manager terminal 105, the mail 1044 of a purport is transmitted by the unauthorized use person, the message of a purport is displayed on the screen of

the manager terminal 105 by the unauthorized use person, and a manager is notified.

[0079] When it is checked that he is the user of normal (step 260), a user is notified of a backup program 1011 through the restoration person terminal 102 so that predetermined wearing opening may be equipped with a tape 100.

[0080] Then, if the attested user equips predetermined wearing opening with a tape 100 according to the operator guidance of a backup program 1011, backup book processing (step 510) will be started.

[0081] In this backup book processing, the volume ID 1001 of a tape 100 is first read through the medium controlling mechanism 1016 (step 511).

[0082] Next, it is directed on the screen of the restoration person terminal 102 that a backup program 1011 inputs a user's cryptographic key (step 512).

[0083] If a cryptographic key is inputted, it will direct to input further two or more restoration persons ID other than the user who carried out the backup process on the screen of the restoration person terminal 102 (step 513).

[0084] A backup program 1011 transmits the inputted cryptographic key to the data encryption program 1013, makes the data which should back up to this encryption program 1013 encipher (step 514), and is made to store in a tape 100 (step 515). In this case, the backup data which should be enciphered are stored in the memory which is not illustrated.

[0085] Next, the data encryption program 1013 performs restoration person registration processing after termination of backup book processing.

[0086] Henceforth, a procedure advances by processing of the data encryption program 1013, and the response of the restoration person authentication server 1043.

[0087] The data encryption program 1013 makes User ID, Volume ID, and the decode person ID input from the restoration person terminal 102 in restoration person registration processing (step 520).

[0088] And User ID is made into an argument and a connection request is transmitted to the restoration person authentication server 1043 through OS1012

and OS1041 (step 521). Under the present circumstances, the restoration person authentication server 1043 will permit connection, if the restoration person DB107 is available (step 551).

[0089] In addition, when the restoration person authentication server 1043 is not started, it waits until it is connectable by retry, or the whole backup process is ended by the time-out. Moreover, the restoration person authentication server 261 performs and (step 552) carries out the reconfirmation certificate of the processing asked to the user authentication server 260 based on a transmitting person's user ID if needed.

[0090] Next, Volume ID and User ID are made into an argument, and the information of a decode key and a restoration person is transmitted (step 522).

[0091] If the restoration person authentication server 1043 receives the information of a decode key and a restoration person (step 553), it will register the decode key and the restoration person ID corresponding to Volume ID and User ID of an inquiry into the restoration person DB107 with reference to the restoration person DB107 (step 554).

[0092] After the data encryption program 1013 checks that the decode key and the restoration person ID have been registered and cuts a session with the restoration person authentication server 1043 (step 523), it cancels transmit data (step 524).

[0093] Since he is trying to register the decode key and the restoration person ID corresponding to Volume ID into the restoration person DB107 on-line, in registration becoming easy compared with the approach of storing and registering into a card record medium according to this operation gestalt, when a card record medium is lost, other restoration persons whom the backup operator accepted can prevent falling impossible [restoration].

[0094] In addition, in step 522,553, if transmit data is enciphered using a data encryption procedure other than a data encryption procedure, surreptitious use of a cryptographic key can be prevented.

[0095] Drawing 6 is a flow chart which shows the procedure which delivers and

receives on-line the cryptographic key of the tape 100 which is a portable medium, and attests a restoration person.

[0096] First, a restoration person starts the restoration program 1017 through the restoration person terminal 102. The restoration program 1017 calls the user check program 1014, in order to check whether a user is a restoration person of normal before starting restoration processing.

[0097] The user check program 1014 calls the user authentication server 1042 of the 2nd calculating machine 104 through the communication facility and the network 103 of OS1012. And a user transmits the user ID who inputted from the restoration person terminal 102.

[0098] The user authentication server 1042 which received User ID acquires these two or more users ID 108 beforehand registered into DB106 from a user DB106. And if it investigates whether there is any match with the user ID who received from the 1st computer 101 and a match is in the user ID 108, the user concerned will attest with his being the user of normal (step 601).

[0099] If the user ID in agreement is not registered, since it is an unauthorized use person, that is notified to the user check program 1014 of the 1st computer 101, and the restoration program 1017 through the communication facility and the network 103 of OS1042, it displays that he is an unauthorized use person on the screen of the restoration person terminal 102, and restoration processing is stopped [subsequent] to the restoration program 1017. Furthermore, to the manager terminal 105, the mail 1044 of a purport is transmitted by the unauthorized use person, the message of a purport is displayed on the screen of the manager terminal 105 by the unauthorized use person, and a manager is notified.

[0100] When it is checked that he is the user of normal, a user is notified of the restoration program 1017 through the restoration person terminal 102 so that predetermined wearing opening may be equipped with a tape 100.

[0101] Then, if the attested user equips predetermined wearing opening with a tape 100 according to the operator guidance of the restoration program 1017, the

restoration program 1017 will detect the volume ID 1001 of a tape 100 through the medium controlling mechanism 1016 (step 602).

[0102] Henceforth, a procedure advances by processing of the restoration program 1017, and the response of the restoration person authentication server 1043.

[0103] The restoration program 1017 performs decode key acquisition processing based on the volume ID 1001 detected at User ID and step 602 which were attested at step 601 (step 610).

[0104] In this decode key acquisition processing, first, User ID is made into an argument and a connection request is transmitted to the restoration person authentication server 1043 through OS1012 and OS1041 (step 611). Under the present circumstances, the restoration person authentication server 1043 will permit connection, if the restoration person DB107 is available (step 651). When the restoration person authentication server 1043 is not started, it waits until it is connectable by retry, or the whole backup process is ended by the time-out. Moreover, the reconfirmation certificate of the restoration person authentication server 1043 is asked and (step 652) carried out to the user authentication server 260 based on a transmitting person's user ID if needed.

[0105] Next, volume ID 1001 and User ID are made into an argument, and a decode key is asked (step 612).

[0106] The restoration person authentication server 1043 searches the decode key corresponding to Volume ID and User ID of an inquiry with reference to the restoration person DB107 (step 653).

[0107] The restoration person authentication server 1043 transmits the decode key of a retrieval result (step 654). In this case, if the corresponding decode key is not registered, the information on to that effect is transmitted.

[0108] After checking that the restoration program 1017 has received the decode key (step 613), a session with a restoration person authentication server is cut (step 614).

[0109] After the restoration person authentication server 1043 transmits the

information on a decode key, it is the approach of deleting the record about the medium which corresponds from the restoration person DB107, and prevents from the decode key of the same medium coming to hand henceforth (step 655).

[0110] When a decode key cannot come to hand, it is judged as a medium with a possibility that it might already be decrypted or might be altered (step 615), and by the approach of outputting that to the screen of the restoration person terminal 102, it warns an operator (step 630) and restoration processing is ended.

[0111] When a decode key is able to come to hand, it progresses to restoration book processing (step 620).

[0112] In restoration book processing, the data encryption program 212 is started by making a decode key into an argument, the data of a tape 100 are read and decrypted (step 621), and restoration to a computer is performed (step 622).

[0113] If someone restores among two or more operators, it can avoid using the same cryptographic key as 2 times by forming step 655 in this restoration procedure.

[0114] Although the above-mentioned example described registration of a restoration person and the approach of authentication, this invention is not limited to this, is and, as for being applicable to the procedure of preventing overwrite to the medium which the others enciphered, does not have an arm, either.

[0115] In case the 3rd operation gestalt drawing 7 of this invention performs a backup process, it is a flow chart which shows the procedure which carries out the automatic check of being the portable medium which the others enciphered on-line.

[0116] First, a user (backup operator) starts a backup program 1011 through the restoration person terminal 102. A backup program 1011 calls the user check program 1014, in order to check whether a user is a user of normal before starting a backup process.

[0117] The user check program 1014 calls the user authentication server 1042 of the 2nd calculating machine 104 through the communication facility and the network 103 of OS1012. And a user transmits the user ID who inputted from the

restoration person terminal 102.

[0118] The user authentication server 1042 which received User ID acquires these two or more users ID 108 beforehand registered into DB106 from a user DB106. And if it investigates whether there is any match with the user ID who received from the 1st computer 101 and a match is in the user ID 108, the user concerned will attest with his being the user of normal (step 701).

[0119] If the user ID in agreement is not registered, since it is an unauthorized use person, that is notified to the user check program 1014 of the 1st calculating machine 101, and a backup program 1011 through the communication facility and the network 103 of OS1042, it displays that he is an unauthorized use person on the screen of the restoration person terminal 102, and a backup process is stopped [subsequent] to a backup program 1011. Furthermore, to the manager terminal 105, the mail 1044 of a purport is transmitted by the unauthorized use person, the message of a purport is displayed on the screen of the manager terminal 105 by the unauthorized use person, and a manager is notified.

[0120] When it is checked that he is the user of normal, a user is notified of a backup program 1011 through the restoration person terminal 102 so that predetermined wearing opening may be equipped with a tape 100.

[0121] Then, if the attested user equips predetermined wearing opening with a tape 100 according to the operator guidance of a backup program 1011, the volume ID 1001 of a tape 100 will be read through the medium controlling mechanism 1016.

[0122] Henceforth, a procedure advances by processing of a backup program 1011, and the response of the restoration person authentication server 1043.

[0123] Next, a backup program 1011 performs medium check processing based on the volume ID 1001 detected at User ID and step 702 which were attested at step 701 (step 710).

[0124] In this medium check processing, first, User ID is made into an argument and a connection request is transmitted to the restoration person authentication

server 1043 through OS1012 and OS1041 (step 711). Under the present circumstances, the restoration person authentication server 1043 will permit connection, if the restoration person DB107 is available (step 751). However, when the restoration person authentication server 1043 is not started, it waits until it is connectable by retry, or the whole backup process is ended by the time-out. Moreover, the reconfirmation certificate of the restoration person authentication server 1043 is asked and (step 752) carried out to the user authentication server 260 based on a transmitting person's user ID if needed.

[0125] Next, volume ID is made into an argument and the user ID corresponding to the volume ID concerned is asked (step 712).

[0126] The restoration person authentication server 1043 searches the user ID corresponding to the volume ID of an inquiry with reference to the restoration person DB107 (step 753).

[0127] The restoration person authentication server 1043 transmits the user ID of a retrieval result to a backup program 1011 (step 754).

[0128] If the user ID corresponding to the volume ID of an inquiry is not registered, the purport of a non-dense is transmitted (step 754).

[0129] A backup program 1011 checks having received the inquiry result (step 713), and cuts a session with the restoration person authentication server 1043 (step 714).

[0130] Next, a backup program 1011 compares the user ID who attested with the user ID who received previously, and when not in agreement, it judges that a tape 100 is the medium which the others enciphered (step 715), and it is the approach of outputting that to the screen of the restoration person terminal 102, and it warns an operator of it (step 730), and it ends a backup process.

[0131] When the user ID who attested with un-registering or the user ID who received previously is in agreement with the restoration person DB107, it judges with it being the medium which the others have not enciphered, and progresses to this processing (step 720) of backup.

[0132] According to the procedure of this example, it can check on-line that a

tape 100 is enciphered by persons other than a user. And the overwrite and the alteration to a tape which the others enciphered can be prevented by checking before backup. Moreover, since User ID is transmitted and received, there is an advantage realizable [with the same protocol as the conventional user authentication].

[0133] In addition, any of a private key method and a open cryptographic key method are sufficient as the approach of encryption used in each above-mentioned example. Since the delivery approach of a key becomes simple especially in the case of a private key method, it is more effective.

[0134]

[Effect of the Invention] While according to this invention enciphering by the cryptographic key as which the backup operator specified the data for backup and storing in a portable medium in case data are backed up to portable media, such as a tape, as explained above ID of two or more restoration persons whom the backup operator permitted "activation of restoration processing", In case Volume ID and the cryptographic key of a portable medium which stored backup data are registered into the restoration person DB and backup data are restored ID of two or more restoration persons who are 1 set in the volume ID of a portable medium Read-out, When it investigates whether the restoration person ID who is in agreement with ID which those who are going to restore inputted exists and the restoration person ID in agreement exists Those who are going to restore attest with his being the restoration person of normal who had "activation of restoration processing" accepted by the backup operator, and are made to allow decode for the encryption data of a portable medium with the decode key transmitted from the decode key or the 2nd calculating machine which the restoration person inputted.

[0135] For this reason, if the backup operator registers into the restoration person DB ID of those who accept "activation of restoration processing" Only the decode person of normal whom the backup operator itself accepted can be made to restore the backup data of a portable medium, without performing troublesome

delivery of a cryptographic key (decode key). Backup data leak to the outsider whom the backup operator does not accept, or it prevents being altered, and it becomes possible to hold the secret nature of backup data, and safety.

[0136] Moreover, batch registration of Volume ID, the restoration person ID, and cryptographic key of a portable medium is carried out by the restoration person DB, and since unitary management is carried out, a system administrator's time and effort can be saved.

[0137] Moreover, since he is trying to send a decode key only once in case the data of a portable medium are decrypted when the identifier of a portable medium and a user's identifier are asked to the restoration person DB and it is attested as a restoration person of normal, a restoration person can save the time and effort which delivers and receives a cryptographic key from a backup operator.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the system configuration Fig. showing the operation gestalt of the distributed system which enforces the data backup approach of this invention.

[Drawing 2] It is the flow chart which shows the procedure of a backup process and restoration processing.

[Drawing 3] It is drawing for explaining the user authentication procedure in restoration processing of drawing 1 .

[Drawing 4] It is drawing for explaining the restoration person authentication procedure in restoration processing of drawing 1 .

[Drawing 5] It is the flow chart which shows the procedure which carries out automatic registration of the restoration person information on-line.

[Drawing 6] It is drawing showing the procedure which delivers and receives the

cryptographic key of a portable medium on online, and attests a restoration person.

[Drawing 7] It is the flow chart which shows the procedure which carries out the automatic check of the portable medium which the others enciphered on-line.

[Description of Notations]

100 [-- Network,] -- A tape, 101 -- The 1st computer, 102 -- A restoration person terminal, 103 104 -- The 2nd computer, 105 -- A manager terminal, 106 -- User DB, 107 -- The restoration person DB, 108 -- User ID, 1001 -- Volume ID 1011 -- A backup program, 1013 -- Data encryption program, 1014 [-- A user authentication server, 1043 / -- A restoration person authentication server, 1082 / -- The restoration person ID, 1083 / -- Cryptographic key.] -- A user check program, 1015 -- A restoration person check program, 1017 -- A restoration program, 1042